Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Pipeline Physical Security: Federal Efforts

May 11, 2023

Securing the nation's energy pipelines from malicious attacks has long been a priority for Congress and federal agencies. The Transportation Security Administration's (TSA) *2020 Biennial National Strategy for Transportation Security* identifies pipelines as vulnerable to cyberattacks and physically "vulnerable to terrorist attacks largely due to their stationary nature, the volatility of transported products, and [their] dispersed nature." After a 2021 ransomware attack against the Colonial Pipeline, Congress focused its attention on pipeline cybersecurity. However, more recent developments, including the 2022 bombing of the Nord Stream pipelines in Europe, physical attacks on the U.S. electricity grid, and a new feature film fictionalizing domestic pipeline terrorism have drawn renewed attention to pipeline physical security.

Evolving Physical Threats to Pipelines

After the terror attacks of September 11, 2001, the federal pipeline security program focused on physical threats from transnational terrorist groups, especially Al Qaeda. This transnational focus has since broadened to include threats from criminal groups and nation-states. Most recently, on May 3, 2023, a NATO intelligence official reportedly warned that Russia was "actively mapping allied critical infrastructure," including pipelines, "on land and on the seabed," and there was a "significant risk" Russia could target this infrastructure in Europe and North America in response to allied support for Ukraine.

A 2011 federal threat assessment (marked Unclassified/For Official Use Only) stated that "domestic extremists" including "environmental activists" were responsible for pipeline "tampering and vandalism" and "likely also pose threats to pipeline networks." Such an incident occurred in 2016 when climate activists temporarily disrupted five pipelines transporting oil from Canada to the United States by closing manual safety valves. In 2017, activists damaged the Dakota Access Pipeline, then under construction. A subsequent Government Accountability Office report stated, "threats to the nation's pipeline systems have evolved to include sabotage by environmental activists." An April 4, 2023, Kansas City Regional Fusion Center security bulletin states that the film, *How to Blow Up a Pipeline*, which depicts domestic climate activists plotting to bomb an oil pipeline, "could potentially inspire similar attacks."

The Department of Homeland Security also has warned about threats to critical energy infrastructure from other violent extremists, including threats to the electricity grid from white nationalists with societal goals. Threats to the grid and threats to pipelines may be linked. In a 2021 report, the North American Electric Reliability Corporation (NERC) stated that, due to growing electric and natural gas system interdependency, industry "should evaluate the need for additional assessments of the risks of ... attacks on midstream or interstate natural gas pipelines."

TSA's Pipeline Security Program

Pipelines are part of the surface transportation critical infrastructure sector, for which TSA is the sector risk management agency and administers the federal program for pipeline security. The Aviation and Transportation Security Act of 2001 (P.L. 107-71), which established TSA, authorizes the agency "to issue, rescind, and revise such regulations as are necessary" to carry out its functions (§101). The Implementing Recommendations of the 9/11 Commission Act of 2007 (P.L. 110-53) directs TSA to promulgate pipeline security regulations and carry out necessary inspection and enforcement if the agency determines that regulations are appropriate (§1557(d)). TSA also cooperates with the Department of Transportation, which also has certain pipeline security authorities, under the terms of a 2006 agreement delineating their respective roles.

Prior to the Colonial Pipeline cyberattack, TSA relied upon industry's voluntary compliance with the agency's guidelines for pipeline physical security and cybersecurity. In 2003, TSA initiated its ongoing pipeline Corporate Security Review Program, wherein the agency conducts voluntary visits with the pipeline operators "to assess the current security practices ... with a focus on the physical and cyber security of pipelines." The agency's reliance on voluntary compliance with recommended security standards had long been questioned by some stakeholders. In 2021, following the Colonial Pipeline incident, TSA issued its first mandatory cybersecurity requirements in the form of a Security Directive applicable to owners and operators of critical pipeline facilities. The agency subsequently issued a second cybersecurity directive and has subsequently revised and replaced both. However, TSA has not similarly imposed mandatory requirements for physical security. Some pipeline companies have publicly reported physical security investments, but such measures remain voluntary.

Congressional Action

In recent years, Congress has acted to strengthen federal efforts to protect pipelines from physical attacks. In the 118th Congress, the Pipeline Sabotage and Accident Prevention Act (H.R. 1484) would mandate fines or imprisonment for causing, or threatening to cause, a defect in equipment to be used in a pipeline facility or for disrupting the operation of a pipeline facility. The Lower Energy Costs Act (H.R. 1), which passed in the House, and the proposed SPUR Act would require the Federal Energy Regulatory Commission (FERC) to consult TSA on the compliance of natural gas pipeline permit applicants with the agency's best practice recommendations regarding pipeline infrastructure security, cybersecurity, and other security measures. In the 117th Congress, the Pipeline Security Act (H.R. 3243) would have recodified TSA's responsibility relating to "securing pipelines against cybersecurity threats, acts of terrorism, and other nefarious acts that jeopardize the physical security or cybersecurity of pipelines." The Energy Product Reliability Act (H.R. 6084) would have required FERC to certify an Energy Product Reliability Organization for pipelines that would establish and enforce pipeline "physical security" standards, among other standards.

As congressional oversight of the federal pipeline security program continues, issues may arise regarding the relative level of TSA and private sector resources dedicated to physical security versus cybersecurity, and whether those resources reflect relative risk. Congress also may consider whether TSA's continued reliance on voluntary guidelines for physical security is appropriate, or whether the agency should impose mandatory physical security requirements as it has for cybersecurity. The quality, quantity, and timeliness of physical threat information originating with the government and being shared with the private sector may also be an area of focus.

Author Information

Paul W. Parfomak
Specialist in Energy Policy

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.